

NSE5_EDR-5.0^{Q&As}

Fortinet NSE 5 - FortiEDR 5.0

Pass Fortinet NSE5_EDR-5.0 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/nse5_edr-5-0.html

100% Passing Guarantee 100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

Instant Download After Purchase

- 100% Money Back Guarantee
- 💿 365 Days Free Update
- 800,000+ Satisfied Customers





QUESTION 1

Refer to the exhibits.

APP	LICATIONS				19
AJI	Mark As	Deiete	Hodfy Action	Advanced Filter	Export V
	APPLICATION		VENDOR	REPUTATION	VULNERABILITY
0	Ø FileZilla	Signed	Tim Kosse	Unknown	Unknown
	⊘ 3.50.0			Unknown	Unknown
D	🕗 FileZilla	Signed	FileZilla Project	Unknown	Unknown
	COLLECTOR GROUP NAME			DEVICE	NAME
Ð	High Security Collector Group (1/1)				
ø	98 DBA (1/1)				
				C80922	31196
D	Default Collector Group (0/0)				



APPLICATION DETAILS		
Policies Policy	Action	
Default Communication Control FORDET		According to policy
	-+I Deny	According to policy
Finance Policy		Manually
Simulation Communication Control Policy	¦→ Allow	According to policy
	→I Deny	According to policy
ASSIGNED COLLECTOR GRO Finance Policy	UPS	

The exhibits show application policy logs and application details Collector C8092231196 is a member of the Finance group What must an administrator do to block the FileZilia application?

- A. Deny application in Finance policy
- B. Assign Finance policy to DBA group
- C. Assign Finance policy to Default Collector Group
- D. Assign Simulation Communication Control Policy to DBA group

Correct Answer: B

QUESTION 2

How does the FortiEDR approach compare to the traditional EDR? (Choose two.)

A. FortiEDR blocks threats in real time, eliminating the response gap



- B. Traditional EDR is faster
- C. There is no difference in response time
- D. FortiEDR requires less staff

Correct Answer: AD

QUESTION 3

What is the purpose of the Threat Hunting feature?

- A. Delete any file from any collector in the organization
- B. Find and delete all instances of a known malicious file or hash in the organization
- C. Identify all instances of a known malicious file or hash and notify affected users
- D. Execute playbooks to isolate affected collectors in the organization

Correct Answer: B

"Threat hunting allows management console users to find and remediate dormant threats before they execute. Essentially it\\'s a search and destroy operation."

QUESTION 4

FortiXDR relies on which feature as part of its automated extended response?

A. Playbooks

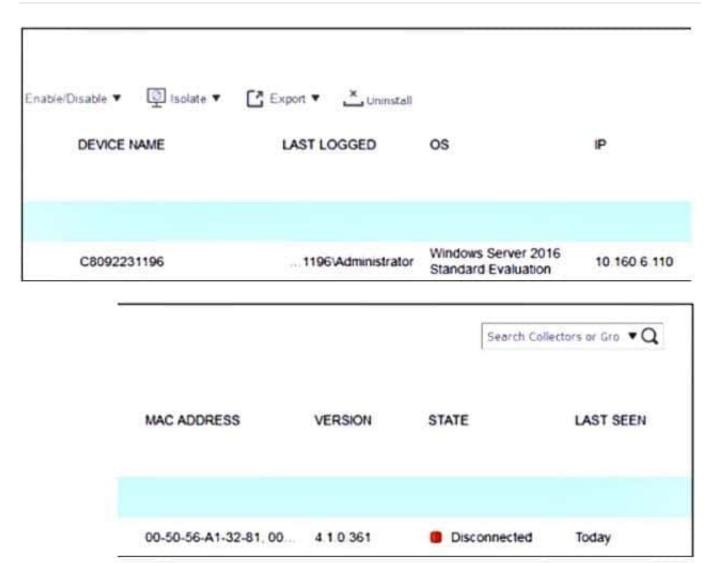
- **B. Security Policies**
- C. Forensic
- D. Communication Control

Correct Answer: A

QUESTION 5

Refer to the exhibits.





Admini	strator: Command Prompt		
C:\Users	\Administrator≻netstat	t -an	
Active C	onnections		
Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:5985	0.0.0.0:0	LISTENING
TCP	0.0.0.0:49692	0.0.0.0:0	LISTENING
TCP	10.160.6.110:139	0.0.0.0:0	LISTENING
TCP	10.160.6.110:50853	10.160.6.100:8080	SYN_SENT
TCP	172.16.9.19:139	0.0.0.0:0	LISTENING
TCP	172.16.9.19:49687	52.177.165.30:443	ESTABLISHED

The exhibits show the collector state and active connections. The collector is unable to connect to aggregator IP address 10.160.6.100 using default port. Based on the netstat command output what must you do to resolve the connectivity issue?



- A. Reinstall collector agent and use port 443
- B. Reinstall collector agent and use port 8081
- C. Reinstall collector agent and use port 555
- D. Reinstall collector agent and use port 6514

Correct Answer: B

Latest NSE5_EDR-5.0 Dumps NSE5 EDR-5.0 Exam Questions

NSE5 EDR-5.0 Braindumps